



# **REPORT**

# **System Hardening via**

# **Local GPO: Windows**

# **Defender**

*v1.0.0*

Author:

**Eldon Gabriel**

October 1, 2025





Cybersecurity Professional | IT Security Consultant

## TABLE OF CONTENTS

<b>REVISION HISTORY.....</b>	<b>2</b>
<b>I. WINDOWS DEFENDER GPO HARDENING.....</b>	<b>3</b>
1.1 Project Description.....	3
1.2 Configuration Summary.....	4
1.3 Validation and Testing.....	4
1.4 Supporting Work.....	4
<b>II. CONCLUSION.....</b>	<b>5</b>
2.1 Key Takeaways.....	5
2.2 Security Implications and Recommendations.....	5








Cybersecurity Professional | IT Security Consultant

## REVISION HISTORY

Version	Date	 Author	Description of Changes
v1.0.0	10/01/2025	Eldon G.	Initial draft.







Cybersecurity Professional | IT Security Consultant

# I. WINDOWS DEFENDER GPO HARDENING

## 1.1 Project Description

This project shows how to set up a Local Group Policy Object (GPO) on a Windows 10 computer. It aims to strengthen the **Windows Defender Antivirus**. The goal was to set important defender options. These options include protection, scanning actions, and preventing users from turning off the antivirus software.



**Disclaimer:** This report documents my personal work completing an MCSI lab exercise. It reflects my understanding and configuration of Windows Defender settings in a controlled, offline environment. No MCSI video or lab materials have been posted, shared, or distributed, ensuring compliance with MCSI's policies.





## 1.2 Configuration Summary

Eleven policies were established using the Local Group Policy Editor (`gpedit.msc`) under **Windows Defender Antivirus**. This study was divided into three main areas.

1. **Core Antivirus Service Control** – Windows Defender remains on and cannot be turned off.
2. **Real-Time and Behavioral Monitoring** – Ensure to scan downloads, archives, and removable media. In addition, it monitors behavior and processes to detect many types of threats.
3. **User Access Restrictions** – Restricting standard users from pausing, disabling, or bypassing antivirus protections.

This setup strengthens security in layers while maintaining ease of use.

## 1.3 Validation and Testing

After applying the Group Policy changes, the system was refreshed using the command:

```
cmd
```

```
gpupdate /force
```

The machine was then restarted to confirm the persistence of the fault. I logged in as a regular user and attempted to change the Windows Defender settings. The test showed that the **Defender Antivirus could not be turned off or avoided**, and all the scanning features remained active.

## 1.4 Supporting Work

1. Compared hardened settings against default Windows Defender behavior to confirm policy impact.
2. Documented configuration categories for portfolio presentation, ensuring no explicit solution disclosure.
3. Verified that system behavior aligned with exercise expectations and novice-level learning objectives.
4. Confirmed persistence of settings after system restart and refresh with `gpupdate /force`.





## II. CONCLUSION

### 2.1 Key Takeaways

- Successfully hardened Windows Defender through Local GPO.
- Three categories of configurations were applied: service control, advanced scanning, and user access restrictions.
- The protections were validated to be persistent and non-removable by a standard user account.

### 2.2 Security Implications and Recommendations

- Using group policies to enforce antivirus protection makes computers safer and more secure. This prevents users from turning off or avoiding antivirus software. This helps protect computers from viruses, phishing, and threats from USB drives.

**Recommendation:** Apply these settings to a domain-level GPO in business settings to protect all devices in the same manner.

---